REMARKS

The Examiner has rejected Claims 1-11, 13-24, and 26 under 35 U.S.C. 102(e) as being anticipated by Bowman-Amuah (U.S. Patent 6,438,594). Applicant respectfully disagrees with this rejection, especially in view of the amendments made hereinabove.

For example, the Examiner relies on the following excerpts to make a prior art showing of applicant's claimed "broadcasting a digitally signed election initiating packet over the network by a sending node in the network, the election packet containing a value for at least one criteria" (see this or similar, but not identical, language in all of the independent claims).

> "Digital Certificates or Signatures-encrypted digital keys that are issued by a third party 'trusted' organization (i.e. Verisign); used to verify user's authenticity." (Column 86 lines 47-49)
>
> "The following are examples of products that perform Transport-level packet filtering: firewalls: Check Point FireWall-1-combines Internet..." (Column 92 lines 20-22)
>
> "...manually searching for content they want and 'pulling' it back to the desktop via a graphical browser. But in the push model, on which subscription servers are based on, content providers can broadcast their information directly to individual users' desktops. The technology uses the Internet's strengths as a two-way conduit by allowing people to specify the type of content they want to receive." (Column 113 lines 14-20)

Such excerpts, however, merely suggest digital signatures for verifying a user, packet filtering, and broadcasting content over the Internet. There is not even a suggestion, however, of any sort of broadcast of a digitally signed election initiating packet, let alone an election initiating packet that contains a value for at least one criteria, as claimed. Only applicant teaches and claims such a specific type of packet with such particular contents for secure automatic selection of a designated service provider in a peer-to-peer network.

Still yet, the Examiner relies on the following excerpt to make a prior art showing of applicant's claimed "awaiting one of expiry of response time-out period and receipt of a response election packet" (see this or similar, but not identical, language in all of the independent claims).

> "Object Messaging enables objects to transparently make requests of and receive responses from other objects located locally or remotely." (Column 79 lines 42-44)

This excerpt, however, merely suggests object messaging. There is not even a suggestion, however, of any sort of awaiting of either a response time-out period or a receipt of a response election packet (as defined in the previous claim element), as claimed. Only applicant teaches and claims such a waiting operation so that a decision can be made based thereon, as claimed.

Even still, the Examiner relies on the following excerpts to make a prior art showing of applicant's claimed "broadcasting a digitally signed election result packet indicating the sending node is the designated service provider if expiry of response time-out period occurs prior to receipt of a response election packet" (see this or similar, but not identical, language in all of the independent claims).

> "...locating a service provider capable of delivering the required service..." (Column 1 line 20)
>
> "Optionally, the determination of which server component is the most appropriate may be preformed by allocating the requests on a round-robin basis whereby requests are assigned to consecutive server components by traversing along the listing of available server components. As another option, the determination of which server component is the most appropriate may also include calculating an amount of utilization that each available server component is currently experiencing." (Column 285 lines 4-12)

After carefully reviewing such excerpts, however, it is clear that it merely suggests the general field of the invention and determining which of a plurality of server components is to be utilized based on a round-robin technique or based on utilization. There is not even a suggestion, however, of any sort of broadcast of an election result packet, let alone an election result packet that indicates that the sending node is the designated service provider, as claimed. Even still, there is not even a mention of any sort of broadcast, specifically if expiry of a time-out period occurs prior to the receipt of a response election packet.

Finally, the Examiner relies on the following excerpt to make a prior art showing of applicant's claimed "awaiting for, verifying, and storing election result in an election result broadcast if receipt of a response election packet occurs prior to expiry of response time-out period" (see this or similar, but not identical, language in all of the independent claims).

> "Optionally, the determination of which server component is the most appropriate may be preformed by allocating the requests on a round-robin basis whereby requests are assigned to consecutive server components by traversing along the listing of available server components. As another option, the determination of which server component is the most appropriate may also include calculating an amount of utilization that each available server component is currently experiencing.
>
> The amount of utilization of each available server components may be calculated base on current CPU utilization, kernel scheduling run-queue length, current network traffic at a node to the server component, and/or a number of requests currently being serviced. Also, a request may be rerouted to a different available server component upon a crash of the selected server component. Additionally, the server components may be saved in a persistent store, wherein a check is made to determine whether a connection to a server component needs to be reestablished." (Column 285 lines 4-22)

This excerpt, however, merely elaborates the above excerpt as to the conditions in which different server components are used, namely based on CPU utilization, network traffic, number or requests, etc. There is not even a suggestion, however, of any sort of verification and storage of an election result in an election results broadcast, let alone of such operation based on the specific condition that a response election packet is received prior to expiry of a response time-out period.

It appears that the Examiner is relying on teachings relating to general concepts of distribution of request allocation among server components. On the other hand, applicant teaches and claims a specific protocol for secure automatic selection of a designated service provider in a peer-to-peer network, namely utilizing the specifically claimed interaction of applicant's claimed election initiating packet, time-out period, response election packet, etc. in the claimed manner involving the particular conditions emphasized hereinabove. This specific, unique protocol provides an improved selection technique.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d

1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

It appears that the Examiner has simply broken down applicant's claim language into components and has then attempted to make a prior art showing of such components in a vacuum. For example, the Examiner points to digital signatures for verifying a user in Bowman-Amuah to meet applicant's claimed "digitally signed election initiating packet." The mere mention of digitally signed user verification is completely out of the context of an election initiating packet, as claimed.

Thus, the Examiner's rejection may be considered analogous to gleaning phrases from applicant's claims, and then using the prior art collectively as a dictionary to make a prior art showing of the same. The Examiner is again reminded that a claim is anticipated only if each and every element as set forth in the claim is found, and the elements must be arranged as required by the claim. *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990).

Despite the aforementioned paramount differences between the claimed invention and the prior art of record and in the interest of expediting the prosecution of the present application, applicant has amended independent Claims 1 and 14 to include the following subject matter of former Claims 2 and 4 et al.:

> "wherein the response election packet contains a value for the at least one criteria;
>
> wherein said verifying election result includes verifying that the value for at least one criteria in the response election packet wins over the value for at least one criteria in the initiating election packet" (see this or similar, but not identical, language in all of the independent claims).

With respect to such former subject matter of Claims 2 and 4 et al., the Examiner relies on the following excerpts to make a prior art showing of such claimed features.

"In order to support scalability in a high volume distributed component environment, resources tend to be replicated. How can incoming requests be distributed amongst the available server components in order to optimize the usage of system resources?

In a distributed system, server components provide functions and data that can be accessed by client components. Many identical copies of a server component can be running on different platforms in the system n order to support large volumes of client requests.

In order to make use of the system's scarce resources, some way f routing an incoming request to the best server component available is required. In general, all requests take a similar length of time to service.

FIG. 150 illustrates server components 15000 receiving service requests 15002.

Therefore, use Load Balancer to select the best server component out of an available pool for the client to use.

FIG. 151 illustrates a load balancer 15100 mediating the requests of FIG 150.

Incoming client requests are routed by the Load Balancer to the best available server component.

A number of possible strategies exist for deciding which server component is the most appropriate at a given point in time.

Round-Robin—Allocate the received requests on a round-robin basis, whereby a list of the available server components is created and, as requests are received, they are allocated by traversing down the list. When the end of the list is reached, the next request is allocated to the server component at the beginning of the list.

Utilization Based—Allocate the received requests base on the utilization that each server component is currently experiencing. The definition of utilization can be tailored to meet specific requirements or deployment strategies. It may be based on a combination of current CPU utilization, kernel scheduling run-queue length, current network traffic at that node, number of requests currently being received, or any other factors particular to the environment." (Column 285 lines 23-63)

"Transport Security 2410

Transport Security services (within the Transport Services layer) perform encryption and filtering.

Transport-layer encryption

Encryption within the Transport Services layer is performed by encrypting the packets generated by higher level services (e.g., Message Transport) and encapsulating them in lower level packets (e.g., Packet Forwarding/Internetworking). (Note that encryption can also occur within the Communications Services layer or the Network Media layer.) Encryption within the Transport Services layer has the advantage of being independent of both the application and the

transmission media, but it may make network monitoring and troubleshooting activities more difficult.

The following standards support transport-layer encryption:
Point to Point Tunneling Protocol
Layer 2 Tunneling Protocol
Transport-layer filtering

Network traffic can be controlled at the Transport Services layer by filtering data packets based on source and/or destination addresses and network service. This ensures that only authorized data transfers can occur. This filtering is one of the roles of a packet filtering firewall. (A firewall is a system that enforces an access control policy between a trusted internal network and an untrusted external network.)

The following IETF standard supports interoperability among security systems:

IPSec Allows two nodes to dynamically agree on a security association based on keys, encryption, authentication algorithms, and other parameters for the connection before any communications take place; operates in the IP layer and supports TCP or UDP. IPSec will be included as part of IPng, or the next generation of IP." (Column 91 lines 19-54)

Such excerpts, however, merely suggest, in a general manner, security technology and various techniques for determining which of a plurality of server components is to be utilized based on a round-robin technique, based on utilization, etc. There is simply no verification by a sending node involving a criteria and value specifically associated with the use of an initiating election packet and response election packet, and the associated conditions, as claimed.

Applicant further emphasizes that independent Claims 9 and 22 include additional detail similar to that set forth above, which may be used to determine whether the receiving node or sending node wins, and is thus deemed allowable for reasons similar to those set forth hereinabove with respect to Claims 1 and 14.

Applicant further notes that the Examiner's application of the prior art to applicant's remaining dependent claims is also replete with deficiencies. Just by way of example, the Examiner relies on the following excerpt to make a prior art showing of applicant's claimed "verifying a digital signature of a response election packet upon receipt of the response election packet prior to expiry of response time-out period" (see Claim 3 et al.).

"Authentication services verify network access requests by validating that users are who they claim to be. For secure systems, one o more authentication mechanisms can be used to validate authorized users and to verify which functions and data they have access to. Within the corporate network, authentication services are often included in directory services products like Novell's NDS. NDS requires the user to have an established account and supply a password before access is granted to resources though the directory.

Authentication for accessing resources across an Internet or intranet is not as simple and is a rapidly evolving area. When building e-commerce Web sites there may be a need to restrict access to areas of information and functionality to known customers or trading partners. More granular authentication is required where sensitive individual customer account information must be protected from other customers." (Column 86 lines 9-25)

Such excerpt, however, merely suggests authorization techniques in the context of user verification. Again, only applicant teaches and claims verification of a digital signature of a response election packet, based on a specific condition, namely upon receipt of the response election packet prior to expiry of a response time-out period.

With respect to Claim 6 et al., the Examiner relies on the following excerpt (and Fig. 96) to make a prior art showing of applicant's claimed "wherein the response time-out period is at least a sum of maximum delay election response period and round trip transmission time."

"connection establishment display—time between the connection request and a confirm being received by the requester." (Column 93 lines 1-3)

Such excerpt, however, merely defines a delay as a time between the connection request and a confirm being received by the requester. Such delay in no way suggests a sum of maximum delay election response period and round trip transmission time, let alone such a specific delay in connection with a time-out period, as claimed.

With respect to Claim 8 et al.. the Examiner relies on the following excerpts to make a prior art showing of applicant's claimed "wherein each of the digitally signed election initiating packet and said digitally signed election result packet is signed by a 1024-bit VeriSign digital certificate."

"CA certificates from both Thawte and Verisign can be utilized." (Column 83 lines 40-41)

Such excerpt, however, merely suggests authorization techniques in the context of user verification. Again, only applicant teaches and claims verification of a digital signature of an election result.

The aforementioned anticipation criterion has simply not been met by the foregoing excerpts. A notice of allowance or a specific prior art showing of each of the foregoing claimed features, in combination with the remaining claimed features, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the following newly claimed subject matter for consideration:

"wherein the at least one criteria includes a plurality of criteria" (see Claim 27);

"wherein the at least one criteria includes node name, MAC (media access control) address, Internet access, bandwidth, operating system, and processor speed" (see Claims 28);

"wherein the at least one criteria includes a plurality of criteria at different levels" (see Claims 29); and

"wherein lower-level criteria break ties associated with higher-level criteria" (see Claims 30).

Again, a notice of allowance or a specific prior art showing of each of the foregoing claimed features, in combination with the remaining claimed features, is respectfully requested.

In conclusion, all of the independent claims are deemed allowable. By virtue of their dependence on such independent claims, all of the remaining claims are further deemed allowable.

Reconsideration is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. For payment of the fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P274_01.013.01).

Respectfully submitted,
Zilka-Kotab, P.C.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
Telephone: (408) 505-5100